
On Brahmagupta's and Kummer's quadrilaterals

K.R. Nagarajan and R. Sridharan

K.R. Nagarajan obtained his Ph.D. from the University of Chicago in 1962. He then served as a professor and later as the head of the School of Mathematics at Madurai Kamaraj University in Tamil Nadu, India, until 1993. Presently, he is a visiting professor at the Chennai Mathematical Institute in Chennai, India.

R. Sridharan obtained his Ph.D. from Columbia University, New York, in 1960. He then served as a professor of the School of Mathematics at the Tata Institute of Fundamental Research in Mumbai, India, until the year 2000. Presently, he is adjunct professor at the Chennai Mathematical Institute in Chennai, India.

Introduction

The Greeks developed geometry as a deductive science, its main results being derived from axioms. The Indians, however, studied geometry in its arithmetic aspects from early times. For instance, construction of right angled triangles with rational sides and hypotenuse was a problem of interest right from the Sulva period in India. In this tradition, Brahmagupta, in the 7th century AD, studied the question of the existence and construction of (cyclic) quadrilaterals whose sides and diagonals are rational. This work came to light to the European mathematicians through the work of Colebrooke [2]. Chasles, the French geometer, was so fascinated by this that he, in fact, included a note on Brahmagupta's work in [1].

Die Suche nach ebenen geometrischen Figuren mit ganzzahligen oder rationalen Seitenlängen und/oder Flächeninhalten hat tiefe historische Wurzeln. Beispielsweise führt die Suche nach rechtwinkligen Dreiecken mit ganzzahligen Katheten und Hypotenuse auf die pythagoräischen Zahlentripel. Ein anderes Beispiel ist das sogenannte Kongruenzzahlproblem aus dem 7. Jh., d.h. die Frage nach der Existenz rechtwinkliger Dreiecke mit rationalen Seitenlängen und vorgegebenem ganzzahligem Flächeninhalt, ein bis heute noch nicht vollständig gelöstes Problem. Im vorliegenden Beitrag geht es um die Existenz von Vierecken mit rationalen Seiten und Diagonalen. Die Autoren erinnern dabei zunächst an Kummers Parametrisierung solcher Vierecke mit Hilfe von rationalen Punkten auf speziellen elliptischen Kurven und diskutieren danach gewisse entartete Fälle, welche in Kummers Arbeit unberücksichtigt blieben.

Kummer, in [6], makes a critical study of the original work of Brahmagupta as explained by Chasles and shows that the existence of rational quadrilaterals (not necessarily cyclic) is equivalent to the existence of rational points of a particular type on certain cubic curves.

We begin this paper with a brief account of the early history of the problem and examine Kummer's method.

Starting with a given rational triangle, Kummer gives an iterative method for constructing infinite families of rational quadrilaterals, using the so called "ascent method" of Euler for the construction of solutions of "canonical" quadri-quadratic equations [7, pp. 255–256]. We note that Kummer has tacitly assumed that the initial rational triangle ABC is the union of two rational triangles ABE and BEC with $AE \neq EC$. If $AE = EC$, we are naturally led to consider the question of existence of rational triangles with a rational median. It turns out that this is equivalent to the existence of rational points of a particular type in the intersection of two quadrics, or equivalently, to the existence of certain rational points for a class of elliptic curves [7].

We show that in the special case where the cosine c of the base angle at the median BE has absolute value $1/3$, the question of existence of such a rational triangle is equivalent to that of the existence of four rational squares in arithmetic progression (considered by Fermat and Euler [7]), which is known to have a negative answer. By using a descent method, we show that the answer is negative also for $|c| = 1/2$.

Throughout this paper, we mostly follow the notation in Kummer [6]. All the curves in this paper are defined over the field \mathbb{Q} of rationals and by a rational point, we mean a point defined over \mathbb{Q} .

We are very thankful to the referee for going through an earlier version of this paper and for suggesting several improvements in the exposition.

1 The beginnings

We shall begin with a brief description of Brahmagupta's method of construction of rational triangles and cyclic rational quadrilaterals. By a *rational triangle* we mean a triangle ABC whose sides AB, BC, CA are rational numbers. Any rational triangle ABC whose area is also rational is obtained through the juxtaposition of two rational right angled triangles ABP and BPC where BP is the altitude of the resulting triangle ABC .

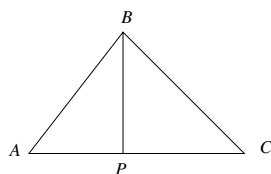


Fig. 1

A quadrilateral $ABCD$ is called *rational* if the sides AB, BC, CD, DA and also the diagonals AC, BD are rational. Brahmagupta gave two constructions for rational cyclic quadrilaterals [3]. In the first method, two rational right angled triangles ABP and BPC

are glued along BP to yield a rational triangle ABC with rational area. Then BP is extended to meet the circumcircle of ABC at D , to yield the cyclic quadrilateral $ABCD$. It is clear that the triangles APD and BPC are similar and, hence, PD is rational. Therefore, $ABCD$ is a rational cyclic quadrilateral (Fig. 2).

In the second method, a rational length AC is chosen and two rational triangles ABC and ADC are constructed with right angles at B and D . The resulting quadrilateral is cyclic and rational (Fig. 3).

Kummer, in [6], notices that the first method can be modified to yield other rational cyclic quadrilaterals. Take first a rational triangle ABC (not necessarily with rational area). Let E be a point on AC such that the triangle ABE is rational. Extend BE to meet the circumcircle of ABC at D . Then, $ABCD$ is a rational cyclic quadrilateral (Fig. 4). In fact, all rational cyclic quadrilaterals are obtained in this way. He also analyses the question of constructing arbitrary rational quadrilaterals starting with rational triangles ABE and BEC .

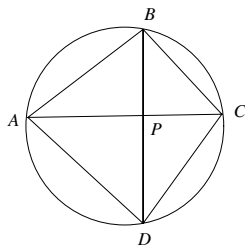


Fig. 2

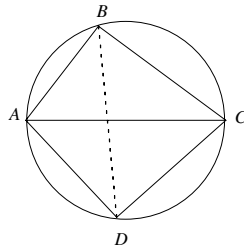


Fig. 3

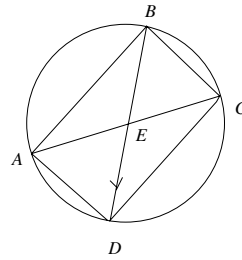


Fig. 4

2 Kummer's parametrisation of rational quadrilaterals through rational triangles

Suppose that ABE is a triangle (see Fig. 5).

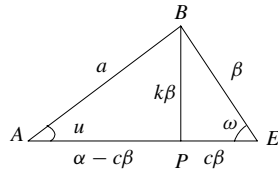


Fig. 5

Let angle $E = \omega$, angle $A = u$, $AB = a$, $BE = \beta$, $AE = \alpha$. Let $c = \cos \omega$. We have $a^2 = \alpha^2 + \beta^2 - 2\alpha\beta c$. Let $a/\beta = x$ and $\alpha/\beta = y$, so that $x^2 - y^2 + 2cy - 1 = 0$. Thus, for a given real value c , with $|c| < 1$, any point (x, y) on the conic $X^2 - Y^2 + 2cY - 1 = 0$, with x and $y > 0$, determines a triangle. This conic is the hyperbola $(X - Y + c)(X + Y - c) = 1 - c^2 = k^2$ where $k = \sin \omega$. Let $\xi \neq 0$ be a real number. Let us define x and y by the equations $x + y - c = \xi$ and $x - y + c = \frac{k^2}{\xi}$. Then, (x, y) is a point on the hyperbola. Since $x = \frac{\xi^2 + k^2}{2\xi}$ and $y = \frac{\xi^2 - k^2 + 2c\xi}{2\xi} = \frac{(\xi + c)^2 - 1}{2\xi}$, if $c \neq 0$ is rational and if ξ is chosen

to be rational and such that both x and y are positive, then ξ determines a triangle ABE the ratio of whose sides are rational. Conversely, any triangle, the ratio of whose sides are rational, is obtained in this way.

If c is rational, $k^2 = 1 - c^2$ is rational. If k is itself rational, the above relates to Brahmagupta's construction of a rational triangle with rational area as a juxtaposition of two rational right triangles.

The problem of constructing a rational quadrilateral can now be posed as follows: Determine successively rational triangles ABE , BEC and CED in such a way that the triangle AED is also rational (Fig. 6).

As a first step, let $c \neq 0$ be a rational number such that $|c| < 1$ and let β be any positive rational number. Let $\xi > 0$ be any rational number such that $(\xi + c)^2 - 1 > 0$. We construct the triangle ABE with $AB = a$, $BE = \beta$, $AE = \alpha$ with

$$\frac{a}{\beta} = \frac{\xi^2 - c^2 + 1}{2\xi} \quad \text{and} \quad \frac{\alpha}{\beta} = \frac{(\xi + c)^2 - 1}{2\xi}.$$

(Then $c = \cos$ of the angle E). Now, suppose that BEC is a rational triangle where $EC = \gamma$ and $BC = b$, $\eta = \frac{b + \gamma - c'\beta}{\beta}$, where $c' = -c$ is the cosine of the angle BEC so that $\eta = \frac{b + \gamma + c\beta}{\beta}$. We then have

$$\frac{b}{\beta} = \frac{\eta^2 - c^2 + 1}{2\eta} \quad \text{and} \quad \frac{\gamma}{\beta} = \frac{(\eta - c)^2 - 1}{2\eta}.$$

(We note that c and the parameter ξ or η determine a triangle up to similarity.)

Since

$$\alpha \left(\frac{\gamma}{\beta} \right) = \gamma \left(\frac{\alpha}{\beta} \right),$$

we have $\alpha[(\eta - c)^2 - 1]\xi - \gamma[(\xi + c)^2 - 1]\eta = 0$. Thus, (ξ, η) is a rational point on the cubic

$$\alpha X[(Y - c)^2 - 1] - \gamma Y[(X + c)^2 - 1] = 0. \quad (*)$$

Suppose that (ξ, η) is a rational solution for $(*)$ so that we have the two rational triangles ABE and BEC . In order to complete the quadrilateral, we need rational triangles AED and CED (Fig. 6).

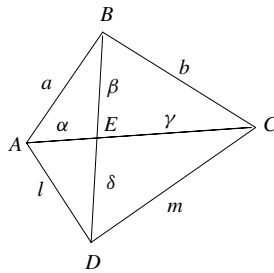


Fig. 6

Let $AD = l$, $DC = m$ and $ED = \delta$. As before, the triangle AED is determined by the rational parameter $x = \frac{l+\delta+c\alpha}{\alpha}$ with

$$\frac{\delta}{\alpha} = \frac{(x-c)^2 - 1}{2x} \quad \text{and} \quad \frac{l}{\alpha} = \frac{x^2 - c^2 + 1}{2x}.$$

Similarly, for the triangle CED taking $y = \frac{m+\delta-c\gamma}{\gamma}$ we should have

$$\frac{\delta}{\gamma} = \frac{(y+c)^2 - 1}{2y} \quad \text{and} \quad \frac{m}{\gamma} = \frac{y^2 - c^2 + 1}{2y}.$$

Then (x, y) should be a rational point on the cubic

$$\alpha Y[(X-c)^2 - 1] - \gamma X[(Y+c)^2 - 1] = 0. \quad (**)$$

Conversely, if (x, y) is a rational point on the cubic (**), such that the corresponding ratios δ/α and δ/γ are positive, then we have the rational triangles AED and CED . Thus, if (ξ, η) is a rational point on the cubic (*) yielding the rational triangle ABC , any rational point (x, y) in (**) which gives a rational triangle ACD will determine a rational quadrilateral $ABCD$.

3 Euler's ascent method

Euler's ascent method is an iterative process of finding a sequence of rational points on a quadri-quadratic curve [7, pp. 255–256].

In general, let $P(X, Y) = 0$ be a polynomial equation over \mathbb{Q} such that P is quadratic in both X and Y . Suppose (x_1, y_1) is a rational point on the curve $P(X, Y) = 0$, so that x_1 is a root of $P(X, y_1) = 0$. This quadratic in X has a second root x_2 . We consider the quadratic equation in Y given by $P(x_2, Y) = 0$. This equation has two roots, one of them being y_1 . Let y_2 be the second root. Then, we return to the first case and consider $P(X, y_2) = 0$ and note that x_2 is a solution of this equation. Let x_3 be the second solution. Then, (x_3, y_2) is also a rational point of the curve. We can continue this process to obtain, *in general*, an infinity of rational points on the curve $P(X, Y) = 0$. However, in particular cases, this process may fold and fail to give an infinite number of solutions.

Kummer applies this method to the cubic (**) for finding rational quadrilaterals. This cubic equation is equivalent to the following (quadratic) equations:

$$\alpha Y X^2 - (\gamma Y^2 + 2c(\alpha + \gamma)Y - \gamma k^2)X - k^2 \alpha Y = 0 \quad (\text{I})$$

and

$$\gamma X Y^2 - (\alpha X^2 - 2c(\alpha + \gamma)X - \alpha k^2)Y - k^2 \gamma X = 0. \quad (\text{II})$$

First note that $X = 0, Y = 0$, is a solution of both (I) and (II); in fact, $X = 0$ if and only if $Y = 0$. Suppose (x_1, y_1) is a rational point on the cubic (I) with $x_1 \neq 0, y_1 \neq 0$. Consider the quadratic equation in X got by substituting $Y = y_1$ in (I). The product of the roots being $-k^2$, we deduce that $(-k^2/x_1, y_1)$ is also a rational point on the cubic. If

we substitute $X = -k^2/x_1$ in equation (II), it can be verified that the resulting quadratic equation is

$$\frac{k^2}{x_1^2}[\gamma x_1 Y^2 - (\alpha x_1^2 - 2c(\alpha + \gamma)x_1 - \alpha k^2)Y - k^2 \gamma x_1] = 0,$$

and has the same roots as when we substitute $X = x_1$ in (II). Therefore, the process folds and yields at most four rational points, (x_1, y_1) , $(-k^2/x_1, y_1)$, $(x_1, -k^2/y_1)$, $(-k^2/x_1, -k^2/y_1)$, starting from any rational point (x_1, y_1) different from $(0,0)$.

In order to get around this difficulty and produce an infinite number of rational points of the cubic, Kummer applies a quadratic transformation by taking $XY = Z$. Multiplying equation (II) by X and substituting $XY = Z$, we get a quadratic equation in Z :

$$\gamma Z^2 - (\alpha X^2 - 2c(\alpha + \gamma)X - \alpha k^2)Z - k^2 \gamma X^2 = 0. \quad (\text{II}')$$

Rewriting this as a quadratic in X , we get

$$(\alpha Z + k^2 \gamma)X^2 - 2c(\alpha + \gamma)ZX - Z(\gamma Z + \alpha k^2) = 0. \quad (\text{I}')$$

For any value x of X , if z, z' are roots of the quadratic equation (II'), then $zz' = -k^2 x^2$ and $z + z' = \frac{\alpha x^2 - 2c(\alpha + \gamma)x - \alpha k^2}{\gamma}$. Also, for any value z of Z , if x, x' are roots of (I'), then, $xx' = -\frac{z(\gamma z + \alpha k^2)}{\alpha z + k^2 \gamma}$ and $x + x' = \frac{2c(\alpha + \gamma)z}{\alpha z + k^2 \gamma}$.

At this point, Kummer takes the initial value $X = 0$. The two roots z, z' of (II') are $z = 0$ and $z' = \frac{-\alpha k^2}{\gamma}$. Substituting $Z = \frac{-\alpha k^2}{\gamma}$ in (I'), we get the two roots $x = 0$ and $x' = \frac{-2c\alpha}{\alpha - \gamma}$. Kummer tacitly assumes $\alpha \neq \gamma$, and proceeds to apply the process iteratively to obtain an infinite sequence of rational points. By choosing particular values for c, α, γ and β , he exhibits infinite sequences of rational quadrilaterals.

This argument obviously breaks down if $\alpha = \gamma$. We treat this case in the next section.

4 Rational triangles with a rational median

Let $\alpha = \gamma \neq 0$. Then we have a rational triangle ABC with a rational median BE (Fig. 7). Let c denote the cosine of the angle ω and let $BE = \beta$.

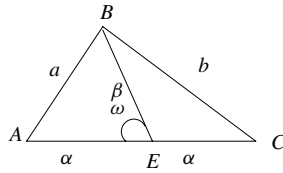


Fig. 7

Let (ξ, η) be the parameters for the triangles ABE and BEC as defined earlier. We then know that (ξ, η) is a point on the cubic (*). This cubic equation can be rewritten as

$$YX^2 - (Y^2 - 4cY - k^2)X - k^2Y = 0, \quad (\text{I}'')$$

and also as

$$XY^2 - (X^2 + 4cX - k^2)Y - k^2X = 0. \quad (\text{II}''')$$

We note that (0,0) is a rational point and that $X = 0$ if and only if $Y = 0$. Let us suppose (x, y) is a rational point on (I'') (or (II'')), such that $x \neq 0, y \neq 0$. Let $y = xt$. Then in (II'')

$$x^3t^2 - x^3t - 4cx^2t + k^2xt - k^2x = 0$$

or

$$x[x^2t^2 - (x^2 + 4cx - k^2)t - k^2] = 0,$$

so that the quadratic equation in $X, T(T-1)X^2 - 4cTX + (T-1)k^2 = 0$ has a rational root $x \neq 0$ for some rational value t of T , which implies, in particular, that $t \neq 0$ or 1 . The discriminant of this equation for $T = t$ is

$$16c^2t^2 - 4(1-c^2)t(t-1)^2 = 4t(1+c)^2(t-\lambda)(1-\lambda t),$$

where $\lambda = (1-c)/(1+c)$. Thus, $4(1+c)^2T(T-\lambda)(1-\lambda T)$ should be a square for some rational value t of T . We have the following:

Proposition 1. *Let ABC be a rational triangle with a rational median BE such that the cosine of the angle $AEB = c$. Let $\lambda = (1-c)/(1+c)$. Let x be the rational parameter associated with the triangle ABE and xt the parameter for the triangle BEC . Then, there is a rational number z such that (z, t) is a rational point on the elliptic curve $Z^2 = 4(1+c)^2T(T-\lambda)(1-\lambda T)$.*

Conversely, suppose (z, t) is a rational point on this elliptic curve and let $x = \frac{4ct \pm z}{2t(t-1)}$. If for one of the values of $x, \frac{(x+c)^2-1}{2x} > 0$, then there exists a rational triangle ABC with rational median BE and cosine of angle $AEB = c$.

Proof. We need only to prove the converse.

If (z, t) is a rational point, the discriminant of the quadratic equation $t(t-1)X^2 - 4cTX + (t-1)k^2 = 0$ is a square. This gives us the rational roots $\frac{4ct \pm z}{2t(t-1)}$. Let x be one of the roots such that $\frac{(x+c)^2-1}{2x} > 0$. Then using the equation $x^2t^2 - (x^2 + 4cx - k^2)t - k^2 = 0$, we get $\frac{(xt-c)^2-1}{2xt} = \frac{(x+c)^2-1}{2x} = \alpha$ say. Then we have rational triangles ABE and BEC such that BE the median of the triangle ABC has length 1 and $AE = EC = \alpha$ and cosine of the angle $AEB = c$. \square

Remark. The elliptic curve given by $Z^2 = T(T-\lambda)(1-\lambda T)$ has the obvious rational points $(0, 0), (\lambda, 0)$ and $(1/\lambda, 0)$, which give 2-torsion points on the elliptic curve. These points yield degenerate cases of the triangle. In case $T = 0$, the corresponding rational point on (II'') is (0,0) which gives the degenerate triangle where $\beta = 0$. If $T = \lambda = (1-c)/(1+c)$, a quick computation gives $X = -(1+c)$ and $Y = -(1-c)$ which will not determine triangles. Similarly, if $T = 1/\lambda$, then $X = 1-c$ and $Y = 1+c$, which will not determine triangles.

We also note the following:

The cosine formulae for the triangles ABE and BEC give the two equations

$$a^2 = \alpha^2 + \beta^2 - 2\alpha\beta c \quad \text{and} \quad b^2 = \alpha^2 + \beta^2 + 2\alpha\beta c.$$

Therefore,

$$b^2 + a^2 = 2(\alpha^2 + \beta^2) = (\alpha + \beta)^2 + (\alpha - \beta)^2$$

and

$$b^2 - a^2 = 4\alpha\beta c = [(\alpha + \beta)^2 - (\alpha - \beta)^2]c.$$

Let $\alpha + \beta = h$ and $\alpha - \beta = g$. We have

$$b^2 + a^2 = h^2 + g^2 \quad \text{and} \quad b^2 - a^2 = (h^2 - g^2)c$$

and, hence,

$$h^2(1 + c) + g^2(1 - c) = 2b^2, \quad (e_1)$$

$$h^2(1 - c) + g^2(1 + c) = 2a^2 \quad (e_2)$$

so that the pair of quadrics in \mathbb{P}^3

$$\frac{(1 + c)}{2}X^2 + \frac{(1 - c)}{2}Y^2 = Z^2 \quad \text{and} \quad \frac{(1 - c)}{2}X^2 + \frac{(1 + c)}{2}Y^2 = T^2$$

intersect at a rational point (x, y, z, t) . Note that $x^2 \neq y^2$.

Conversely, suppose (x, y, z, t) is a rational point in the intersection of the quadrics, such that $x^2 \neq y^2$. Then, by retracing the steps, we can produce a rational triangle with a rational median. We have, therefore, proved the following:

Proposition 2. *The following are equivalent:*

- (1) *There exists a rational triangle ABC with rational median AE and with the cosine of the base angle at $E = c$.*
- (2) *Let $|c| < 1$. The pair of quadrics (F, G) in \mathbb{P}^3 , where*

$$F : \frac{(1 + c)}{2}X^2 + \frac{(1 - c)}{2}Y^2 - Z^2 = 0,$$

$$G : \frac{(1 - c)}{2}X^2 + \frac{(1 + c)}{2}Y^2 - T^2 = 0,$$

has a rational point (x, y, z, t) such that $x^2 \neq y^2$ in its intersection.

Remark 1. Rational points (x, y, z, t) with $x^2 = y^2$ give rise to degenerate triangles.

Remark 2. Let $D(t)$ be the discriminant of the pencil $F - tG$ of quadrics. It can be checked that

$$D(t) = \frac{(1 + c)^2}{4}t(t - \lambda)(1 - \lambda t).$$

The curve Ω in \mathbb{P}^3 defined by the pair of quadrics F and G has the obvious rational points given by $X^2 = Y^2 = Z^2 = T^2$. Hence, by the proposition in [7, p. 136], it follows that the curve Ω is isomorphic to the curve $Z^2 = D(t)$ which is the elliptic curve defined in Proposition 1 above.

5 Rational squares in arithmetic progression

A solution to the problem of finding three rational squares in arithmetic progression was already known to the Greeks. This question is equivalent to that of finding rational pythagorean triples. In fact, if x^2, y^2, z^2 are in arithmetic progression, then we have $y^2 = \frac{1}{2}(x^2 + z^2) = \left(\frac{z+x}{2}\right)^2 + \left(\frac{z-x}{2}\right)^2$, so that $\left(\frac{z+x}{2}\right)^2, \left(\frac{z-x}{2}\right)^2, y^2$ is a pythagorean triple. Conversely, if u^2, v^2, y^2 is a pythagorean triple, then, taking $z = u + v$ and $x = u - v$, we see that x^2, y^2, z^2 are in arithmetic progression.

Motivated by the above Fermat (see [7, p. 149]) raised the question of the existence of four distinct rational squares in arithmetic progression. Euler gave a proof in 1780 that such a foursome does not exist. However, as pointed out by A. Weil (see [7, p. 115]), the first satisfactory proof (based on "descent method") was given by Itard¹ (see [5, p. 112]). Weil also indicates another proof using properties of curves of genus 1 (see [7, p. 147]).

We shall show that the existence of a rational triangle ABC , with rational median BE and cosine of angle $AEB = \frac{1}{3}$, is impossible by showing that this problem is equivalent to the four squares problem.

Proposition 3. *The existence of a rational triangle with a rational median and such that the cosine of the base angle at the median is equal to $\pm 1/3$ is equivalent to the existence of four rational squares in a nontrivial arithmetic progression. Hence, there is no such triangle.*

Proof. We appeal to our earlier theorem. In equations (e_1) and (e_2) , if we substitute $c = 1/3$, we get the two equations

$$2h^2 + g^2 = 3b^2 \quad \text{and} \quad h^2 + 2g^2 = 3a^2.$$

Hence,

$$3b^2 - 3a^2 = h^2 - g^2 \quad \text{and} \quad b^2 + a^2 = h^2 + g^2,$$

so that

$$2b^2 - a^2 = h^2 \quad \text{and} \quad 2a^2 - b^2 = g^2,$$

i.e., g^2, a^2, b^2, h^2 are in arithmetic progression. Conversely, if g^2, a^2, b^2, h^2 are in arithmetic progression, we see by retracing the steps that the equations (e_1) and (e_2) hold with $c = 1/3$. \square

Remark. If $c = 1/2$, the corresponding diophantine equations for a, b are $3a^2 - b^2 = 2x^2$ and $3b^2 - a^2 = 2y^2$. One can prove the nonexistence of rational solutions in this case also (excepting the trivial case $a^2 = b^2 = x^2 = y^2$) by following the method adopted in Weil (see [7, pp. 141–149]).

On the other hand, the method of Fermat's descent can be applied to give a direct proof of the result.

Proposition 4. *The system of equations*

$$3b^2 - a^2 = 2z^2, \quad 3a^2 - b^2 = 2w^2,$$

has no integral solution other than the obvious ones $a^2 = b^2 = z^2 = w^2$.

¹We thank Michel Waldschmidt for sending us a copy of the relevant pages of the book by Itard.

Hence, there are no rational triangles ABC with rational median BE and such that the cosine of the base angle at the median is equal to $\pm 1/2$.

Proof. Suppose there is an integral solution $\{a, b, z, w\}$ and such that not all a^2, b^2, z^2, w^2 are equal. It is easy to see that in this case $b \neq 0$ and $a \neq 0$.

We may assume that a and b are coprime. We also assume that $a, b > 0$ and among all integral solutions $\max(a, b)$ is the least possible value.

Let $A = a/b, B = b/a, W = w/a,$ and $Z = z/b$. We rewrite the equations as

$$A^2 + 2Z^2 = 3, \quad (1)$$

$$B^2 + 2W^2 = 3. \quad (2)$$

We find rational parametrizations of these equations. Let $Z = 1 + t(A - 1)$. Substituting in equation (1) we have the quadratic equation in A :

$$(1 + 2t^2)A^2 + 4(t - t^2)A + 2t^2 - 4t - 1 = 0.$$

Since $A = 1$ is a root, the other root is $\frac{2t^2 - 4t - 1}{1 + 2t^2}$ and the corresponding value for Z is

$$\frac{-2t^2 - 2t + 1}{1 + 2t^2}.$$

Let $t = \lambda/\mu$ where λ, μ are coprime integers. Since a and b are coprime, it follows that for some integer k ,

$$\begin{aligned} ka &= 2\lambda^2 - 4\lambda\mu - \mu^2, \\ kb &= \mu^2 + 2\lambda^2, \\ kz &= \mu^2 - 2\lambda\mu - 2\lambda^2. \end{aligned} \quad (3)$$

Since $\mu^2 + 2\lambda^2 > 0$, we have $k > 0$. It can be easily checked that k is a divisor of 6.

From equation (2) it follows that there exist integers p, q coprime to each other, and a positive integer k' such that

$$\begin{aligned} k'a &= q^2 + 2p^2, \\ k'b &= 2p^2 - 4pq - q^2, \\ k'w &= q^2 - 2pq - 2p^2. \end{aligned}$$

(It can be checked that k' is a divisor of 6.) Therefore, we have

$$\begin{aligned} k'(2\lambda^2 - 4\lambda\mu - \mu^2) &= k(q^2 + 2p^2), \\ k'(\mu^2 + 2\lambda^2) &= k(2p^2 - 4pq - q^2). \end{aligned}$$

Adding and subtracting these equations, we have

$$\begin{aligned} k'\lambda(\lambda - \mu) &= kp(p - q), \\ k'\mu(\mu + 2\lambda) &= -kq(q + 2p). \end{aligned} \quad (4)$$

If k is even, then in view of equations (3), μ is even. Further, if k' is odd, then $\lambda(\lambda - \mu)$ must be even, and, hence, λ or $\lambda - \mu$ and, therefore, λ must be even, a contradiction to our assumption that λ and μ are coprime. Thus, k is even (by symmetry) if and only if k' is even. We may cancel the factor 2 from k and k' and assume that they are both odd. Suppose first that $k = k'$. Cancelling k from equations (4), we have

$$\begin{aligned}\lambda(\lambda - \mu) &= p(p - q), \\ \mu(\mu + 2\lambda) &= -q(q + 2p).\end{aligned}$$

Let $p/\lambda = x$ and $\mu/\lambda = \theta$. We then have from the above the following quadratic equation for θ :

$$\theta^2(x^2 + 1) + 2\theta(3x^2 - 1) + (3x^2 - 1)(x^2 - 1) = 0.$$

The discriminant of this equation is

$$4x^2(3x^2 - 1)(3 - x^2),$$

which should be the square of a rational number, so that $(3x^2 - 1)(3 - x^2)$ must be a square. Let $x = c/d$, where c and d are coprime positive integers. (x can be assumed to be positive.) An easy verification shows that

$$3c^2 - d^2 = 2X^2, \quad 3d^2 - c^2 = 2Y^2,$$

where X and Y are both odd integers.

Thus, (c, d, X, Y) is a solution of equations (1) and (2). Further, since c and d are coprime, with $c/d = p/\lambda$ we have $c \leq p$ and $d \leq \lambda$. From the equation

$$q^2 + 2p^2 = ka,$$

it follows that $p < a$ and, hence, $c < a$ (since $k = 1$ or 3). Similarly, from

$$\mu^2 + 2\lambda^2 = kb,$$

we have $d < b$. By Fermat's descent, we are through in this case.

Let us, therefore, assume that $k \neq k'$ and without loss of generality that $k = 3$ and $k' = 1$. It follows from equations (4) that 3 divides $\lambda - \mu$ and, hence, also $\lambda + 2\mu$. Let $3u = \lambda - \mu$ and $3v = \lambda + 2\mu$. Then, we have

$$\begin{aligned}2\lambda^2 - 4\lambda\mu - \mu^2 &= 3(5u^2 + 2uv - v^2), \\ \mu^2 + 2\lambda^2 &= 3(3u^2 + 2uv + v^2).\end{aligned}$$

Hence, by equations (4), we have

$$\begin{aligned}5u^2 + 2uv - v^2 &= q^2 + 2p^2, \\ 3u^2 + 2uv + v^2 &= 2p^2 - 4pq - q^2.\end{aligned}$$

Adding and subtracting these equations, we have

$$\begin{aligned}u^2 - v^2 &= q^2 + 2pq, \\ 2u^2 + uv &= p^2 - pq.\end{aligned}$$

As before, if $p/u = y$ and $v/u = \sigma$, we have the following quadratic equation:

$$\sigma^2(1 + y^2) + 4\sigma(1 - y^2) + (3y^4 - 9y^2 + 4) = 0,$$

the discriminant of which is $4y^2(3y^2 - 1)(3 - y^2)$ which should be the square of a rational number. Let $y = c/d$, where c and d are coprime integers. We get the following equations:

$$3c^2 - d^2 = 2X^2, \quad 3d^2 - c^2 = 2Y^2,$$

where X and Y are both odd integers. Note that $c/d = p/u$, so that $c \leq p$ and $d \leq u$. From the equation

$$q^2 + 2p^2 = a,$$

it follows that $p < a$ and, hence, $c < a$. Similarly, $d < b$, so that we are through once again by Fermat's descent. This proves the proposition. \square

Rational parallelograms

Dickson (in [4]) gave a complete solution to the problem of finding all rational parallelograms. This is equivalent to finding all rational triangles one of whose medians is rational. (We may assume that all the lengths are integers.) With the notation as in Section 4, we have $a^2 + b^2 = g^2 + h^2$. Dickson has given conditions such that a, b, g, h take integral values. We quickly describe his method below.

Let $a + g = mq$ and $b + h = nq$, where $q = \text{g.c.d. of } a + g \text{ and } b + h$, so that $(m, n) = 1$. Then, there exists an integer p such that $a - g = np$ and $h - b = mp$, so that

$$a = \frac{1}{2}(mq + np), \quad g = \frac{1}{2}(mq - np),$$

$$b = \frac{1}{2}(nq - mp), \quad h = \frac{1}{2}(nq + mp).$$

It easily follows from this that

- (i) if m and n are odd, then p and q have the same parity;

and

- (ii) if only one of m and n is odd then p and q are both even.

Suppose for such an "integer" triangle with an "integer" median, one of the angles at the base of the median has cosine $= 1/3$. From the pair of equations $a^2 = \alpha^2 + \beta^2 - \frac{2}{3}\alpha\beta$ and $b^2 = \alpha^2 + \beta^2 + \frac{2}{3}\alpha\beta$, it follows that $\frac{b^2 - a^2}{h^2 - g^2} = \frac{1}{3}$. This implies

$$8mnpq = (m^2 - n^2)(p^2 - q^2),$$

which should be impossible in view of Proposition 3 proved above. Perhaps, one could prove directly under conditions (i) and (ii) for m, n, p, q that there are no solutions.

References

- [1] Chasles, M.: *Aperçu historique sur l'origine et développement des méthodes en géométrie*. Paris 1875, 436.
- [2] Colebrooke, H.T.: *Algebra, Arithmetic and Mensuration from the Sanskrit of Brahmagupta and Bhāskara*. London 1817.
- [3] Datta, B.; Singh, A.N.: *History of Hindu Mathematics*. A Source Book, I & II, Asia Publishing House, 1962.
- [4] Dickson, L.E.: Rational triangles and quadrilaterals. *Amer. Math. Monthly* 28 (1921), 244–250.
- [5] Itard, J.: *Arithmétique et Théorie des Nombres*. P.U.F., Paris 1973.
- [6] Kummer, E.E.: Über die Vierecke, deren Seiten und Diagonalen rational sind. *J. Reine Angew. Math.* 37 (1848), 1–20.
- [7] Weil, A.: *Number Theory. An Approach through History*. Birkhäuser Verlag, second printing, 1987.

K.R. Nagarajan and R. Sridharan
Chennai Mathematical Institute
92 G.N. Chetty Road
T. Nagar, Chennai-600 017, India
e-mail: nagaraj@cmi.ac.in, rsridhar@cmi.ac.in